

# Method for mutual authentication of an IC-card and a terminal.

**Patent number:** EP0552392  
**Publication date:** 1993-07-28  
**Inventor:** HEWEL HARALD DIPL-ING (DE); KRUSE DIETRICH DIPL-ING (DE); GEFROERER STANISLAUS DIPL-MATH (DE)  
**Applicant:** SIEMENS NIXDORF INF SYST (DE)  
**Classification:**  
 - international: G07F7/10; H04L9/32  
 - european: G07F7/10E; H04L9/32; G07F7/10D4E2  
**Application number:** EP19920101016 19920122  
**Priority number(s):** EP19920101016 19920122

Also published as:

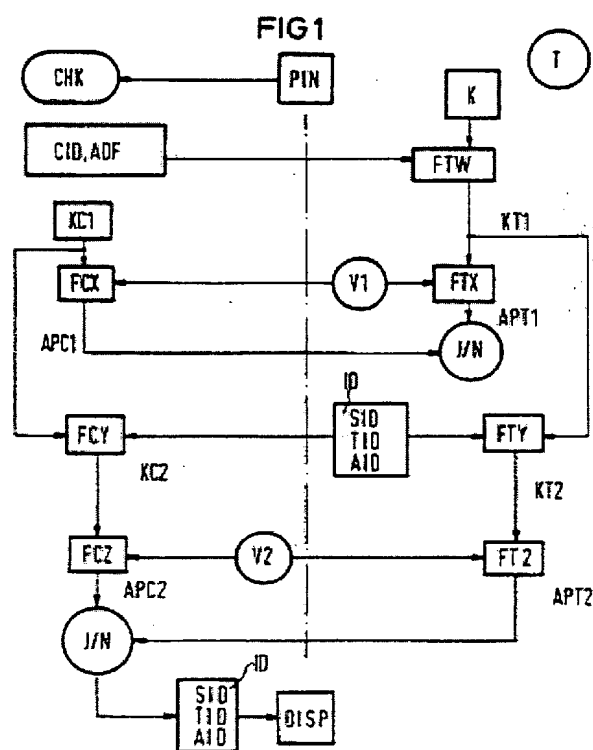
EP0552392 (B1)

Cited documents:

EP0388700  
 EP0400441  
 GB2144564  
 GB2227111  
 XP000095908

## Abstract of EP0552392

The method specified complements the challenge and response method for mutual authentication of a chip card (CHK) and of a terminal (T). A terminal-specific key (KC2, KT2) is calculated with the aid of identity characteristics (ID) for the terminal (T), the current application and the security module located in the terminal (T), a coding function (FCY, FTY) and the chip-card-specific key (KC1, KT1) prior to authenticity testing of the terminal (T). The identity characteristics (ID) are signalled visually and/or acoustically to the chip-card user after successful conclusion of the authenticity test.



Data supplied from the esp@cenet database - Worldwide

BEST AVAILABLE COPY